

(19) World Intellectual Property
Organization
International Bureau



(43) International Publication Date
29 January 2004 (29.01.2004)

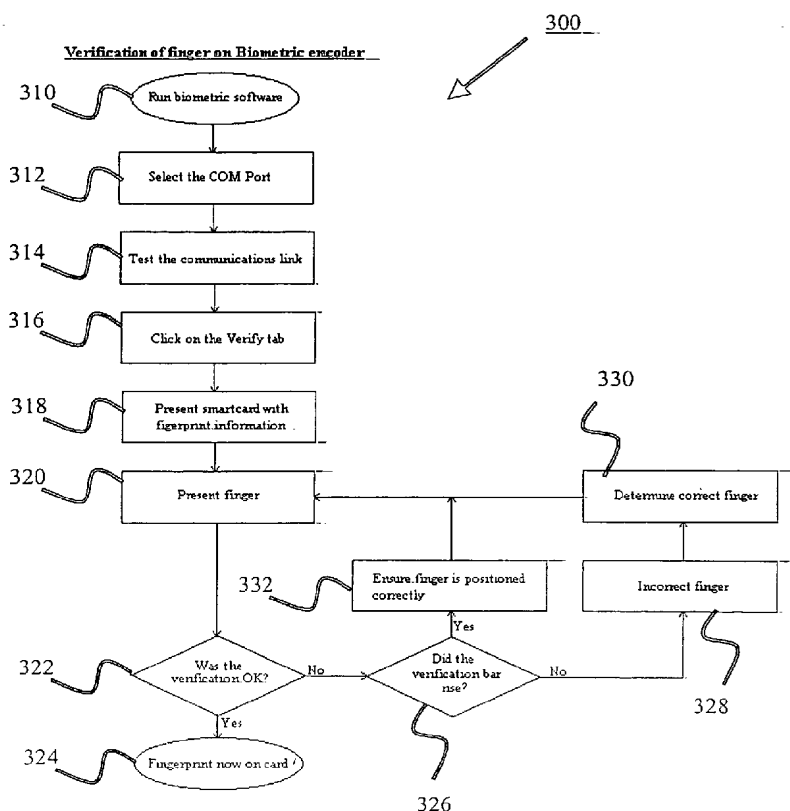
PCT

(10) International Publication Number
WO 2004/010372 A1

- (51) International Patent Classification⁷: **G06K 19/07** (74) Agent: SPRUSON & FERGUSON; GPO Box 3898, Sydney, NSW 2001 (AU).
- (21) International Application Number:
PCT/AU2002/000984
- (22) International Filing Date: 24 July 2002 (24.07.2002)
- (25) Filing Language: English
- (26) Publication Language: English
- (71) Applicant (for all designated States except US):
BANQUE-TEC INTERNATIONAL PTY LTD
[AU/AU]; Unit 5, 12-18 Victoria Street East, Lidcombe, NSW 2141 (AU).
- (72) Inventor; and
- (75) Inventor/Applicant (for US only): **BLAKE, Christopher, Ian** [AU/AU]; Banque-Tec International, Unit 5, 12-18 Victoria Street, East Lidcombe, NSW 2141 (AU).
- (81) Designated States (*national*): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZM, ZW.
- (84) Designated States (*regional*): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: BIOMETRIC SMARTCARD SYSTEM AND METHOD OF SECURE TRANSMISSION



(57) Abstract: Secure transmission systems and security systems utilising biometric sensors are disclosed. A smartcard encoded with details of biometric data is read, and actual biometric data is sensed. The biometric data from the smartcard is then compared with the sensed biometric data. Access may be allowed if the biometric data from the smartcard and the sensed biometric data match. The process may involve verifying the biometric data encoded on the smartcard is correct. The smartcard stores the biometric data after a source of biometric data is scanned and the scanned biometric data is encoded. In a further aspect, secure transmissions are enabled from a smartcard reader. To do so, a signal obtained by the reader dependent on the smartcard is encrypted. The encrypted signal is transmitted to a remote location relative to the reader. At the remote location, the transmitted signal is translated to another format usable by a controller. Access is controlled by the controller dependent upon the translated signal.



Published:

— with international search report

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

BIOMETRIC SMARTCARD SYSTEM AND METHOD OF SECURE TRANSMISSION

Field of the Invention

5 The present invention relates generally to security systems and in particular to secure transmission systems and security systems utilising biometric sensors.

Background

Existing security systems are of several different types. One type of security
10 system utilises a smartcard as a key for access to a secure location or secure equipment. The smartcard contains security information providing access via a smartcard reader at the access point. A user presents the reader with the smartcard. If the smartcard is authorised, the reader actuates a control mechanism to provide access. Thus, for example, the reader may signal a controller that controls operation of a latch mechanism controlling
15 access to a door or provide access to a computer terminal. One example of a relevant reader that may be used in such a system is a Wiegand reader. One significant disadvantage of such systems is that the smartcard if stolen or otherwise in the possession of an unauthorised person may allow the unauthorised person to access the secure location or equipment.

20

Another security system utilises a biometric sensor to control access. A user must provide biometric data, normally a fingerprint, speech, or an eye scan via a sensor at the access point. Other forms of biometric data include facial details and hand geometry. Biometrics is a physical characteristic of a person used as a form of identification. The
25 biometrics data is used in place of, or in addition to a security key, such as a key, card or PIN. A database or central repository of stored biometric data is maintained in a computer, with which the sensor can communicate. The scanned biometric data is compared with the stored biometric data, and if a match is found the user is permitted access. This system is generally more secure than that of the smartcard system, but is
30 disadvantageous in that a central repository of biometric data must be maintained and updated. Further, significant time may be required to conduct such a comparison of the scanned biometric data against the database or central repository to determine whether or not there is a match.

Conventional systems are also disadvantageous in that the products' sizes are bulky. Still a further disadvantage of conventional systems is that such products cannot protect against security breaches arising from a person getting into security lines in a wall to which the reader is connected and providing false authorisation signals and the like to a controller.

Summary

In accordance with a first aspect of the invention, identification using of biometric data is disclosed. A smartcard encoded with biometric data is read. Actual biometric data is sensed. The biometric data from the smartcard is then compared with the sensed biometric data for verification. Access may be allowed if the biometric data from the smartcard and the sensed biometric data match. This may involve verifying that the biometric data encoded on the smartcard is correct. The biometric data stored in the smartcard is derived by scanning a source of biometric data associated with the smartcard, encoding the scanned biometric data, and storing the encoded biometric data on the smartcard. The biometric data may include a fingerprint. Optionally, a detail level can be specified for scanning the biometric data.

In accordance with a second aspect of the invention, a method of providing secure transmissions from a reader is disclosed. A signal created by the reader is encrypted. The encrypted signal is transmitted to a remote location relative to the reader. At the remote location, the transmitted signal is translated to another format usable by a controller. Access is controlled using the controller dependent upon the translated signal.

Brief Description of the Drawings

A small number of embodiments are described hereinafter with reference to the drawings, in which:

Fig. 1 is a high-level flow diagram illustrating an enrolment operation of a biometric smartcard system including a biometric smartcard reader or encoder in accordance with an embodiment of the invention;

Fig. 2 is a flow diagram illustrating a process of enrolling a fingerprint on a smartcard using a biometric smartcard encoder, providing further details of the embodiment of Fig. 1;

Fig. 3 is a flow diagram illustrating a process of verifying a finger on the biometric smartcard encoder, providing further details of the embodiment of Fig. 1;

Fig. 4A is a block diagram illustrating the structure of storage or memory in a smartcard in accordance with the embodiment of the invention;

Fig. 4B is a table illustrating an arrangement of security keys used in the smartcard of Fig. 4A in accordance with the embodiment of the invention;

Fig. 5 is a functional block diagram showing modules of a biometric smartcard reader or encoder in accordance with the embodiment of the invention;

Fig. 6 is a perspective view of a biometric smartcard reader or encoder in accordance with the embodiment of the invention shown in Fig. 5;

Fig. 7 is a block diagram of a secure transmission system in accordance with a further embodiment of the invention; and

Fig. 8 is a flow diagram illustrating a process of secure transmission in accordance with the further embodiment of the invention, which may be practiced with the system of Fig. 7.

Detailed Description

A method, an apparatus, and a system for biometric smartcard reading and encoding, as well as for secure transmissions are described hereinafter. Numerous specific details are set forth. However, it will be apparent to those skilled in the art in the light of this disclosure that various modifications may be made without departing from the scope and spirit of the invention. Embodiments of the invention provide equipment that synthesise biometric and smartcard technologies to provide a smartcard reader or encoder that eliminates central database communications infrastructure. As the smartcard holds the biometric information, the requirement of central repositories of biometric data and associated security issues are obviated. A significant application of the reader or encoder is as an access control device at security point, whether for access via a door or other portal, or to a computer, network, or other secure equipment or installation.

- 4 -

In the following description, the terms biometric smartcard reader and biometric smartcard encoder are used. A reader is a device that is able to scan a person's biometric data and contactlessly read a smartcard to obtain stored biometric data. The biometric data is preferably a fingerprint. The smartcard is presented to the reader (preferably, 10 mm to 40 mm away), and write/read operations are communicated from the reader to the smartcard. The reader then compares the scanned biometric data and stored biometric data to determine if there is a match. The reader may be located at an access point to provide access to a location or equipment in a security system dependent on the results of the comparison. An encoder is able to perform the functions of a reader including contactless communications with the smartcard, but also is able to encode a smartcard with personal details and biometric data. More particularly, the encoder preferably includes a logical access system where all access in a facility is controlled using a card, i.e. for doors, for PC access, etc. Such a smartcard access system by its nature almost ensures that the user does not forget to leave the smartcard behind. Preferably, an encoder has an appropriate interface to enable the encoder to be connected with a computer to enrol a person's details and biometric data on the smartcard using software running on the computer. The encoder stores biometric data in a two-dimensional structure or template and card holder details on the smartcard. The encoder may have an insert slot in the housing body to receive such a smartcard. The slot allows detection of the smartcard during an encoding process. A reader cannot be used for enrolment of biometric data and other associated information on a smartcard as can an encoder. For ease of description, the following text uses the two terms biometric smartcard reader and biometric smartcard encoder substantially interchangeably, but the noted distinctions should be borne in mind.

Biometric Smartcard Reader or Encoder

In accordance with an embodiment of the invention, a biometric smartcard reader or encoder is disclosed. Fig. 5 is a block diagram illustrating a smartcard 540 and a biometric smartcard reader 500 in accordance with an embodiment of the invention. This biometric smartcard reader 500 is smaller than other biometric units. The biometric smartcard reader 500 includes a biometric sensor 510 coupled to a sensor control module or printed circuit board 520. The sensor PCB 520 contains modules for processing and encoding scanned biometric data into a suitable digital representation using a given

coding algorithm (e.g., Sagem). The fingerprint is stored as a template preferably and not as a digital image. An algorithm is used to generate the template. For fingerprints, examples of relevant algorithms use minutiae reference points, or ridge recognition patterns, for example. In turn, the sensor PCB 520 is coupled to a smartcard reader PCB 530 and sends fingerprint data in a given template to the smartcard reader PCB 530, which is also able to interrogate and obtain data from a smartcard 540. This is preferably done by presenting the smartcard reader PCB 530 with the smartcard 540, in which the smartcard reader PCB 530 energises the smartcard 540 if in close proximity and communicates with the smartcard 540. Preferably, the smartcard reader PCB 530 is a contactless reader using a Philips Chip Mifare® utilising the Wiegand format for its output. Communication between the smartcard 540 and the smartcard reader PCB 530 is encrypted. The encryption utilised with this embodiment involves a proprietary encryption method of Mifare®, which is embedded in the Mifare® smartcards. Another option is to use DES encryption. However, it will be apparent to those skilled in the art in the light of this disclosure that other encryption techniques may be used without departing from the scope and spirit of the invention.

More preferably, the biometric smartcard reader 500 incorporates a biometric finger scan sensor 510 (e.g., for scanning fingerprints) with an accompanying sensor PCB 520. The fingerprint sensor technology may be optical, capacitive, thermal, tactile, or a combination of the foregoing. An example of a sensor arrangement that may be used is a Bioscrypt product provided by Bioscrypt Inc. including an Authentic sensor, a Bioscrypt PCB, and Bioscrypt's own encoding algorithm. Alternatively, the sensor arrangement may be implemented using an ST sensor, a Yuean PCB provided by Yuean Biometrics, and the Sagem algorithm, or a SecuGen product provided by SecuGen Corporation including a SecuGen sensor, a SecuGen PCB, and the SecuGen algorithm. Still further, a SecuGen optical solution may be practiced that enables a rugged and robust design. However, it will be apparent to those skilled in the art in the light of this disclosure that other biometric sensors may be practiced without departing from the scope and spirit of the invention. The sensor 510 and associated PCB 520 scan a person's fingerprint and generate a digital representation of that fingerprint as digital biometric data. Fig. 6 is a perspective view of a biometric smartcard reader 600, which embodies the reader 500 of

- 6 -

Fig. 5 including a biometric sensor 610/510, an associated sensor PCB 520 (not shown), and a Mifare® smartcard reader PCB 530 (not shown) in a single unit.

The smartcard 540 is adapted to store a digital representation of the biometric data. Preferably, the smartcard is a Mifare® smartcard for use with the contactless Mifare® reader. The smartcard 540 has approximately 1 Kbyte of storage or memory. Fig. 4A is a block diagram illustrating the structure of the storage 400 in the Mifare® smartcard, which is organised into 16 separate sectors 410-414 – 0 sector 410, 1 sector 412, ..., 15 sector 414. Each of the sectors 410-414 has two keys, Key A and Key B as shown in Fig. 4B. These keys can be designated as read and read/write keys. The keys A and B for each sector are initialised by the manufacturer (e.g. 10 hexadecimal characters each) and can be changed when the sectors are written to to contain biometric data in accordance with the embodiment of the invention. Each Mifare® smartcard 540 also has a unique serial number or identifier. Preferably, the 15th sector 414 contains one or more of the following security parameters for use in the system of Fig. 5: a facility code, a company code, an access code, and an issue code. The facility code can identify a facility that the smartcard permits access to for a given entity or company, which is identified by the company code. The issue code identifies how many smartcards have been issued to a person. For example, if the issue code is 3, the system may hotlist corresponding smartcards for the person with issue codes of 1 or 2.

Dependent upon the format of the digital biometric data, the smartcard 540 stores such data across two or more sectors with corresponding keys for each sector of data. In the preferred embodiment, 5 to 6 sectors are used to store a digital fingerprint representation or template. For example, an ST sensor and an Yuean PCB produces a digital fingerprint representation that is approximately 320 bytes long. The length of the representation may vary depending on the different biometric sensor products and algorithms used. As noted above, each sector needs a customer specific key to unlock the information.

Optionally, the reader 500/600 incorporates a tamper switch so that if a reader is pulled from a wall, the reader does not function and an alarm flag is activated.

- 7 -

As described in greater detail below, use of the biometrics smartcard encoder 500 enables authorised persons using a properly enrolled smartcard to access to a secure location or equipment, for example. Lost or stolen smartcards 540 are unusable as the person with the lost or stolen smartcard 540 does not have the correct biometrics data (e.g., fingerprint) to match that stored on the smartcard 540. Still further, another advantage of this embodiment is that the biometric smartcard reader 500 of Fig. 5 obviates the need for a central database or repository of biometric data, since the biometrics data is stored on the smartcard 540.

In combination with a computer (not shown), a biometrics smartcard encoder 500 can also be used to enrol a person's fingerprint on a smartcard 540. The biometrics smartcard encoder 500 uses an RS232 or USB communications port, in conjunction with software, to enrol the person's fingerprint onto the smartcard 540. Generally, software or a computer program(s) running on the computer in combination with the biometrics smartcard encoder 500 obtains personal details for a person, scans and records a fingerprint for the person, and then writes the personal details and fingerprint representation to the smartcard 540. Preferably, this embodiment does not permit fingerprint information to travel to the computer. Instead, the biometric smartcard encoder 500 stores the information and writes the information directly to the smartcard 540. The information is then erased from the memory of the biometric smartcard encoder 500. When enrolling a person's fingerprint, the detail level for scanning by the biometric smartcard encoder 500 can be changed to enable persons with scarred hands or other aberrations to use the encoder 500. This process is set forth in greater detail with reference to Fig. 1.

25

Fig. 1 is a high-level flow diagram illustrating details of a process 100 of obtaining and storing biometric information in a smartcard 540 using the biometric smartcard encoder (i.e., biometric unit) 500/600. In state 110, the biometric smartcard encoder 500 is initially idle. In step 112, a command is sent to the biometric smartcard encoder 500 to capture a person's fingerprint. This is preferably done by the computer using a communications port. In step 114, the sensor 510/610 of the biometric smartcard encoder 500 captures a fingerprint image. The sensor 510/610 analyses the scanned fingerprint and creates an image. In step 116, the image is coded and the data to be stored

is created. This is preferably done by the sensor PCB 520 in combination with the sensor 510. In step 118, the smartcard 540 is presented to the smartcard reader PCB 530, and the biometric data from the sensor PCB 520 is written into the smartcard 540 by the smartcard reader PCB 530. State 120 at the end of the process 100 shows that the digital fingerprint representation is stored on the smartcard 540. This smartcard 540 can then be used as a security key in relation to a biometric security system.

Generally, when verification or access is required using a biometric smartcard reader 500/600, the smartcard 540 is presented to the biometric smartcard reader 500/600 and the fingerprint information is read off the smartcard 540 by the biometric smartcard reader 500/600. The person then presents their finger to the sensor 510/610 of the biometric smartcard reader 500/600 for scanning. The fingerprint representation read off the smartcard 540 is compared by the biometric smartcard reader 500/600 with the fingerprint currently obtained using the sensor 510/610. If there is a match within the detail level set at enrolment, the biometric smartcard reader 500/600 checks access privileges using the access code from the smartcard 540 and if the holder has appropriate access privileges, access is granted by the biometric smartcard reader 500/600 to the smartcard holder. Verification is strongly dependent on enrolment. A score of 100 applies for a high quality and content template. A medium threshold level may look for a score of 60, for example. The threshold level may be varied to adjust quality and content of a template.

Details of Enrolment Process

Fig. 2 is a more detailed flow diagram of a process 200 of enrolling a fingerprint using a biometric smartcard encoder, based on Fig. 1. In an initial state 210, a biometric software application is run or launched. As noted above, this software is run on a computer connected to a biometric smartcard encoder 500/600, preferably using a RS232 or USB communications port. In step 212, a relevant RS232 or USB port (denoted generally by COM in Fig. 2) is selected by the software. Other interfaces may be practiced without departing from the scope and spirit of the invention. In step 214, the communications link (COM port) is tested to ensure the communications link is operating properly. Communication between the smartcard reader PCB 530 and the computer is preferably triple DES or Skipjack encrypted. Therefore, the information sent for access to

the computer is highly difficult to compromise. In step 216, enrolment of a person's fingerprint is commenced. Preferably, this is done by clicking on an enrolment tab in the software application to commence enrolment processing. In step 218, personal details of the person whose fingerprint is to be enrolled are obtained and the type of smartcard
5 being written to is specified. The relevant information may include one or more of the person's name, facility code, company code, access code, and issue code. Alternatively, the smartcard may be pre-encoded with some or all of this information.

In step 220, the desired detail level of the fingerprint is specified using the
10 software application. In particular, this is done using a quality meter in the software where the detail level for the sensor 510 and PCB 520 is specified. Ordinarily, the quality is set as high as possible to avoid misreads. However, the quality can be adjusted downwardly to avoid or reduce the effects of scar tissue and other aberrations on the person's finger. In step 222, the person's fingerprint is presented to the sensor 510/610 of
15 the biometric smartcard encoder 500/600, and the person's fingerprint is scanned. The data stream for the scanned fingerprint is sent from the sensor 510/610 to the sensor PCB 520. The information is then coded with the specific algorithm within the sensor PCB 520. The coded information is then sent to the smartcard reader PCB 530 and from there encoded onto the smartcard 540.

20 In decision block 224, a check is made to determine if the quality of the scanned fingerprint image from the sensor 510/610 is adequate. The sensor 510 and PCB 520 determines quality. The biometric smartcard encoder 500/600 indicates this to the computer, since the fingerprint is preferably not transferred to the computer. If the
25 quality is inadequate (NO), the quality is reduced to enable enrolment in step 226 and processing continues at step 222. This may occur multiple times. If decision block 224 determines that the quality is adequate (YES), processing continues at step 228.

In step 228, a smartcard 540 is presented to the smartcard reader PCB 530 of the
30 biometric smartcard encoder 500/600. Presentation of the smartcard 540 to the smartcard reader PCB 530 results in the encoded fingerprint template and related keys for each sector being downloaded onto the smartcard 540. The communication between the smartcard 540 and the reader PCB 530 is encrypted. As noted above, the encrypted,

- 10 -

encoded fingerprint representation is normally stored across several sectors in the storage of the smartcard. Also personal details and other information may be stored on the smartcard 540. In step 230, a check is made to determine if the encoding of the smartcard 540 was successful. If decision block 230 returns true (YES), the fingerprint template has
5 been encoded successfully on the smartcard 540 using the encoder 500. If decision block 230 returns false (NO), processing continues at decision block 232. In decision block 232, a check is made to determine if the smartcard type details are correct. For example, the smartcard 540 may be a new or used smartcard. A new smartcard has default values in its storage, while a used smartcard has changed keys A and B for example. Further, or
10 alternatively, a different type of smartcard may be used, for example, from different manufacturers. If decision block 232 returns false (NO) indicating the card type details are incorrect, processing continues at step 234 and the correct smartcard type must be specified to the software. Processing then continues at step 236. If decision block 232 returns true (YES), processing continues at step 236. In step 236, another smartcard is
15 tried or obtained for presentation instead of the smartcard previously presented to the smartcard reader PCB 530 of the encoder 500/600. Processing then continues at step 228.

Details of Verification Process

After a fingerprint representation and associated information are enrolled on a
20 smartcard 540, verification of the enrolment on the smartcard 540 may be required. Fig. 3 is a flow diagram illustrating a process 300 of verifying a fingerprint scanned by the biometric smartcard encoder 500/600 and enrolled on the smartcard 540. In state 310, the biometric application software is loaded. In step 312, the communications link (COM port or USB) between the computer and the biometric smartcard encoder 500 is selected.
25 In step 314, the communications link is tested to ensure the link is operating properly. In step 316, a verification application module in the software is activated. Preferably, this is done by clicking on a verify tab in the biometric application software. In step 318, the smartcard 540 with enrolled fingerprint information is presented to the encoder 500/600, which reads and stores the fingerprint information from the smartcard 540. In step 320,
30 the person's finger is presented to sensor 510/610 of the biometric smartcard encoder 500, and the person's fingerprint is scanned and stored. The biometric smartcard encoder 500 then compares in the smartcard reader PCB 530 the scanned fingerprint template from the sensor 510/610 and the uploaded fingerprint template from the smartcard 540.

- 11 -

In decision block 322, a check is made to determine if the verification passed (OK). The encoder 500/600 provides the comparison result to the computer to establish verification. If decision block 322 returns true (YES), processing continues at state 324 and the fingerprint on the smartcard is verified as that of the fingerprint obtained at the sensor 510/610. Otherwise, if decision block 322 returns false (NO), processing continues at step 326. In step 326, a check is made to determine if the verification bar in the software was raised. Preferably, a quality bar and a verification bar showing current levels are depicted graphically to an operator of the application software on opposite sides of a graphical image of a fingerprint icon, which indicates to the operator when a fingerprint has been properly scanned by the encoder 500/600. Raising the verification bar indicates a better match between the scanned fingerprint and the one from the smartcard 540. Verification is dependent on the quality level at enrolment. If decision block 326 returns true (YES), processing continues at step 332 and the finger must be positioned correctly for verification, before processing continues at step 320. Otherwise, if decision block 326 returns false (NO), processing continues at step 328. A determination is made that the incorrect finger has been used in relation to the recorded fingerprint information on the smartcard. In step 330, the correct finger is determined before proceeding to step 320.

Secure Transmission System

In a security system, a smartcard reader may be setup to give access on a per door basis or to equipment. The smartcard has unique keys that must also be contained in a smartcard reader's firmware. The smartcard reader communicates with the smartcard and information is read from the smartcard for access. The smartcard reader ordinarily communicates with an access controller, and this controller controls access; for example the controller may preferably activate a door latch for access. Information is sent to the controller. Communication between the smartcard reader and the controller is usually Wiegand. However, the communications may be RS485 or RS232. Still further, another example of a common form of communication back to a controller is Clock and Data. These formats can be cracked or defeated given time, as formats are usually 'known' industry standards. The controller determines whether or not to grant access and activates an access mechanism if granted. When using a security access reader to grant or deny

access, a possible breach in security lies in the information that is directly sent to the controller by the smartcard reader. If the smartcard reader is removed from a wall or other connection point and a signal is introduced to the line between the smartcard reader and the controller, then a security breach exists. The signal may provide information to the controller so that the controller improperly grants access. If the smartcard reader has a tamper switch, a degree of added security is provided. A hole in the wall may still be made conditional to the material of the wall, and a security breach may still occur, as this enables access to the cables of the reader. In contrast, a stand-alone reader does not need a controller so this does not apply to such a reader.

In accordance with a further embodiment of the invention, secure transmission from a smartcard reader is provided by encrypting the messages from the smartcard reader in the security system. Preferably, the smartcard reader is a biometrics smartcard reader 500/600, but ordinary smartcard readers may be practiced. The further embodiment of the invention shown in Figs. 7 and 8 addresses this issue.

Fig. 7 is a block diagram of a secure transmission system 700 in accordance with the further embodiment of the invention. A smartcard reader 702 is coupled to a high security module (HSM) 704. Preferably, the smartcard reader 702 is a biometrics smartcard reader 500/600, but may be a standard smartcard reader. The HSM 704 is located remotely from the smartcard reader 702 and preferably at an inaccessible location relative to the smartcard reader 702, for example on the other side of a wall in a secure area. The distance between the smartcard reader 702 and the HSM 704 may be up to 15 metres. Communications between the reader 702 and the HSM 704 are preferably Triple DES or Skipjack encrypted, but other encryption techniques may be employed. The HSM 704 is in turn coupled to a controller 706. Communications between the HSM 704 and the controller 706 are carried out using the controller-specified format, which is usually Wiegand format but may be another format (e.g., clock and data). In turn, the controller 708 is connected to the door latch 708 to control operation of the door for access. Different access mechanisms may be used in place of a door latch 708, for example to provide access to a computer.

Significantly, the system 700 uses an HSM 704 for each access point and encrypted communications between the smartcard reader 702 and the HSM 704. The smartcard reader 702 preferably reads the information off a smartcard and communicates with the HSM 704 on the secure side of the wall, up to 15 metres away. Again, the communication is encrypted, preferably using a 3DES or Skipjack encrypted protocol. The HSM 704 decrypts the message to obtain the security information from the smartcard, e.g. "Facility Code" and the "Access number", and communicates these values to the access controller 706. Thus, communication between the smartcard reader 702 and the HSM 704 and thus the controller 706 is secure whether the smartcard reader 702 is removed from the wall or wiring is accessed through a wall. This provides a higher standard of security for access control systems.

Fig. 8 is a flow diagram illustrating a process 800 for secure transmission. In state 810, the smartcard reader 702 is in standby mode. In step 812, a smartcard is presented for access. In step 814, the smartcard reader 702 reads and analyses access information on the smartcard. The smartcard and the reader must have the same keys. If a standard smartcard reader is used, an encrypted transmission is sent to the HSM 704 in step 816. Processing then continues at step 824. Otherwise, if a biometric smartcard reader 500/600 is used, after step 814, processing continues at step 818. In step 818, biometric data is obtained from the cardholder using the biometric sensor of the biometric smartcard reader 500/600 as reader 702. Preferably, the biometric data is fingerprint information. In step 820, the biometric data of the cardholder and the stored biometric data from the smartcard are compared and confirmed to be the same person or not. If the biometric data matches, in step 822, an encrypted transmission for access is sent to the HSM 704 from smartcard reader 702, before processing continues at step 824. In step 824, the HSM 704 decrypts the transmission and communicates it to the controller 706 using the appropriate controller format, e.g. Wiegand. The controller 706 either grants access 828 in step 826 or denies access 832 in step 830 dependent upon the access rights obtained from the smartcard.

A small number of embodiments of the invention regarding methods, devices, and systems for biometric smartcard reading and encoding, as well as for secure transmissions have been described. In the light of the foregoing, it will be apparent to

- 14 -

those skilled in the art in the light of this disclosure that various modifications may be made without departing from the scope and spirit of the invention.

Claims

The claims defining the invention are as follows:

- 5 1. A method of identification using biometric data, said method including the steps of:
 reading a smartcard encoded with biometric data;
 sensing actual biometric data;
 comparing said biometric data from said smartcard with said sensed biometric
10 data identification.
2. The method according to claim 1, further including the step of allowing access if said biometric data from said smartcard and said obtained biometric data match.
- 15 3. The method according to claim 1, further including the step of verifying said biometric data encoded on said smartcard is correct.
4. The method according to claim 1, further including the step of enrolling biometric data on said smartcard.
20
5. The method according to claim 4, wherein said enrolling step further includes the steps of:
 scanning a source of biometric data associated with said smartcard;
 encoding said scanned biometric data; and
25 storing said encoded biometric data on said smartcard.
6. The method according to claim 1 or 5, wherein said biometric data includes a fingerprint.
- 30 7. The method according to claim 5, further including the step of specifying a detail level for scanning said biometric data.

- 16 -

8. An apparatus for identification using biometric data, said apparatus including:

means for reading a smartcard encoded with biometric data;

means for sensing actual biometric data;

5 means for comparing said biometric data from said smartcard with said sensed biometric data.

9. The apparatus according to claim 8, further including means for allowing access if said biometric data from said smartcard and said biometric data
10 obtained at said access point match.

10. The apparatus according to claim 8, further including means for verifying said biometric data encoded on said smartcard is correct.

15 11. The apparatus according to claim 8, further including means for enrolling biometric data on said smartcard.

12. The apparatus according to claim 11, wherein said enrolling means further includes:

20 a biometric scanner for scanning a source of biometric data associated with said smartcard;

means for encoding said scanned biometric data; and

a smartcard reader for storing said encoded biometric data on said smartcard.

25 13. The apparatus according to claim 8 or 12, wherein said biometric data includes a fingerprint.

14. The apparatus according to claim 12, further including means for specifying a detail level for scanning said biometric data.

30

15. A method of providing secure transmissions from a smartcard reader, said method including the steps of:

- 17 -

encrypting a signal created by said smartcard reader dependent on said smartcard;
transmitting said encrypted signal to a remote location relative to said reader;
translating at said remote location said transmitted signal to another format
5 usable by a controller;
controlling access using said controller dependent upon said translated signal.

16. The method according to claim 15, wherein said smartcard contains biometric data and said smartcard reader includes a biometric smartcard reader for
10 obtaining biometric data directly.

17. The method according to claim 16, wherein said biometric data includes fingerprint data.

15 18. An apparatus for providing secure transmissions from a smartcard reader, said apparatus including:

a smartcard reader for encrypting a signal created by said smartcard reader dependent on said smartcard;

20 means for transmitting said encrypted signal to a remote location relative to said smartcard reader;

means for translating at said remote location said transmitted signal to another format;

a controller for controlling access using dependent upon said translated signal.

25 19. The apparatus according to claim 18, wherein said smartcard contains biometric data and said smartcard reader includes a biometric smartcard reader for obtaining biometric data directly.

30 20. The apparatus according to claim 19, wherein said biometric data includes fingerprint data.

- 1/7 -

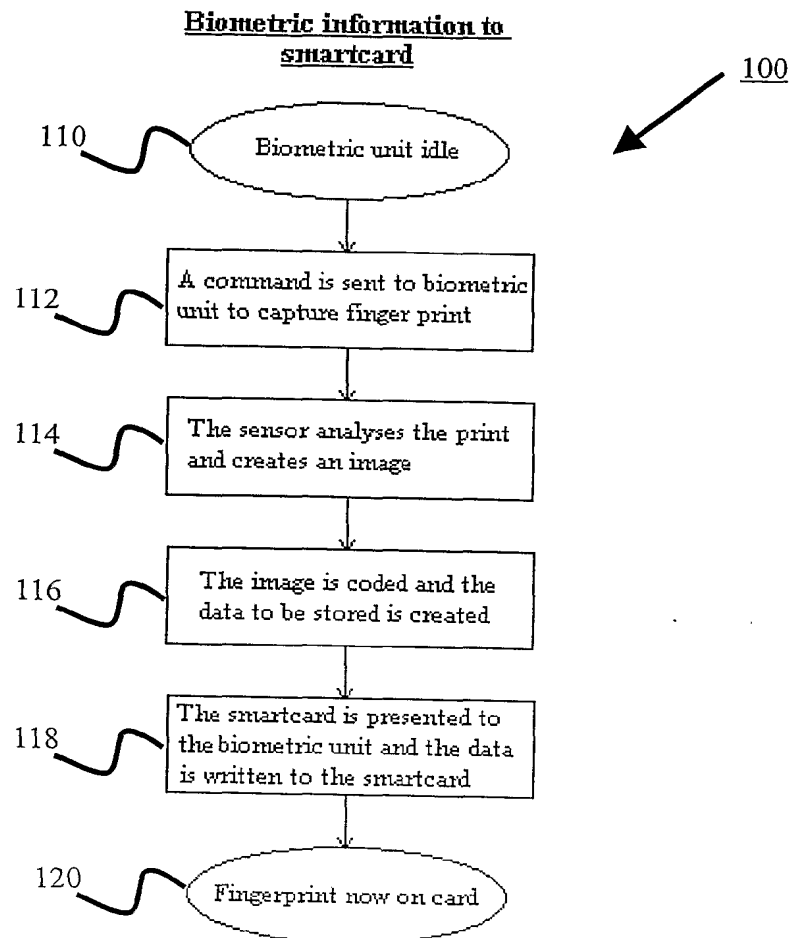


FIG. 1

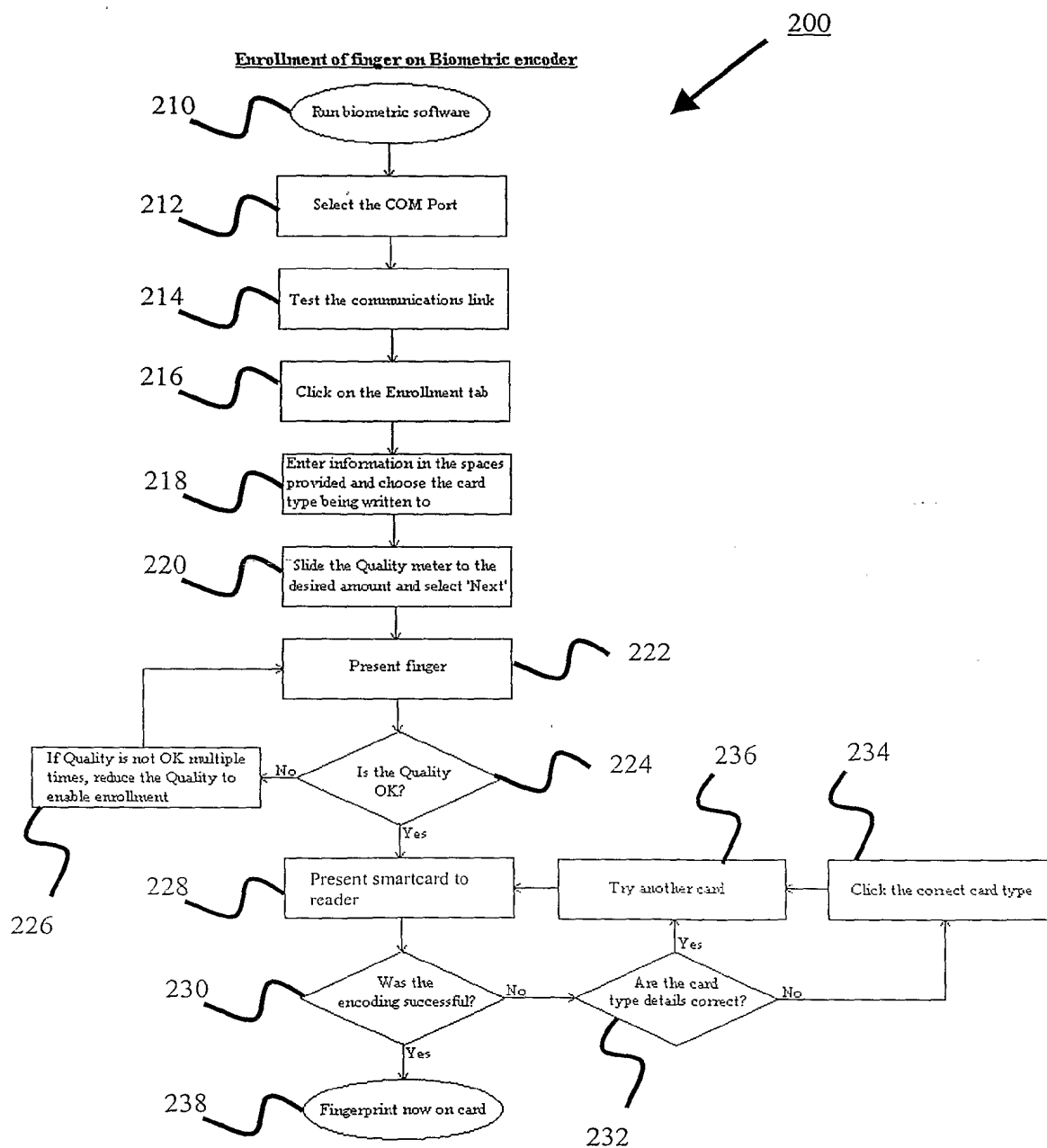


FIG. 2

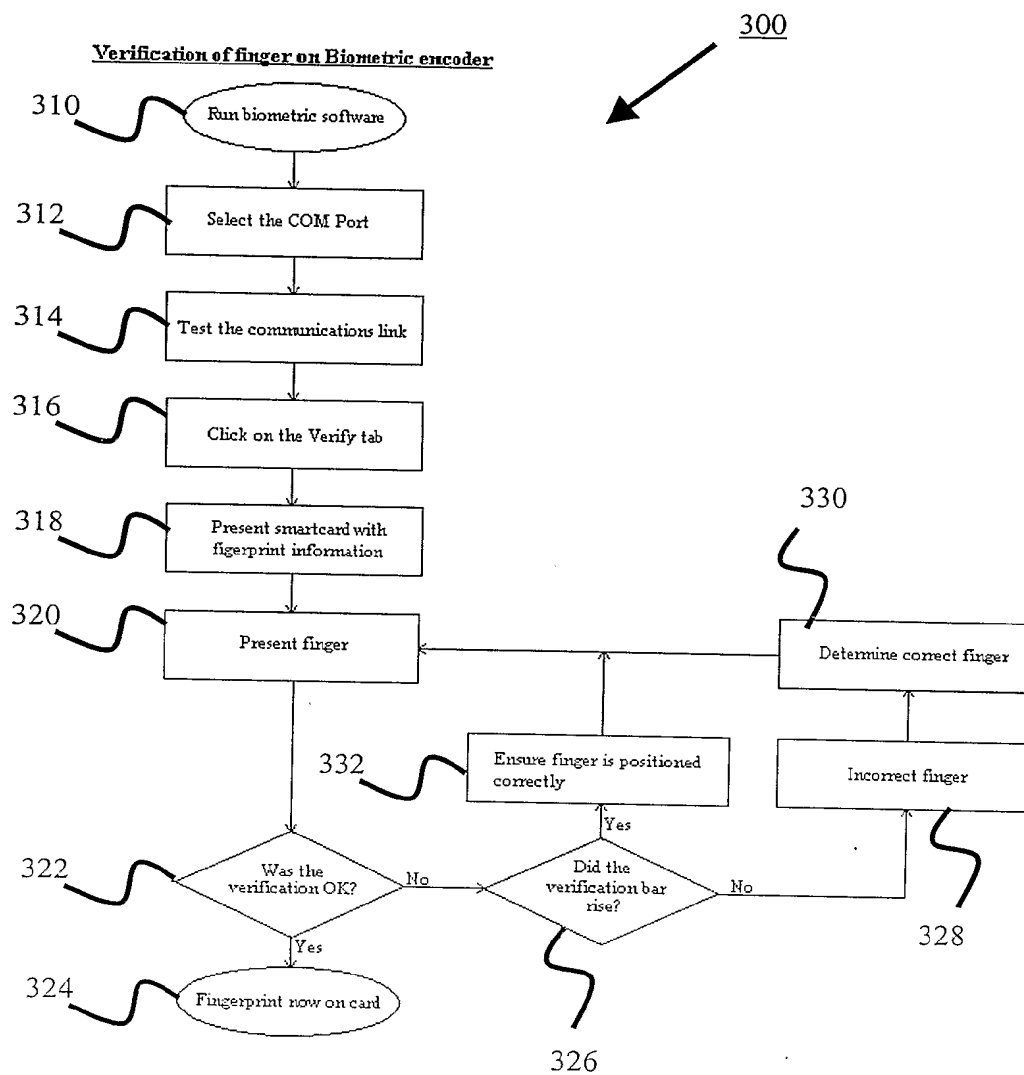


FIG. 3

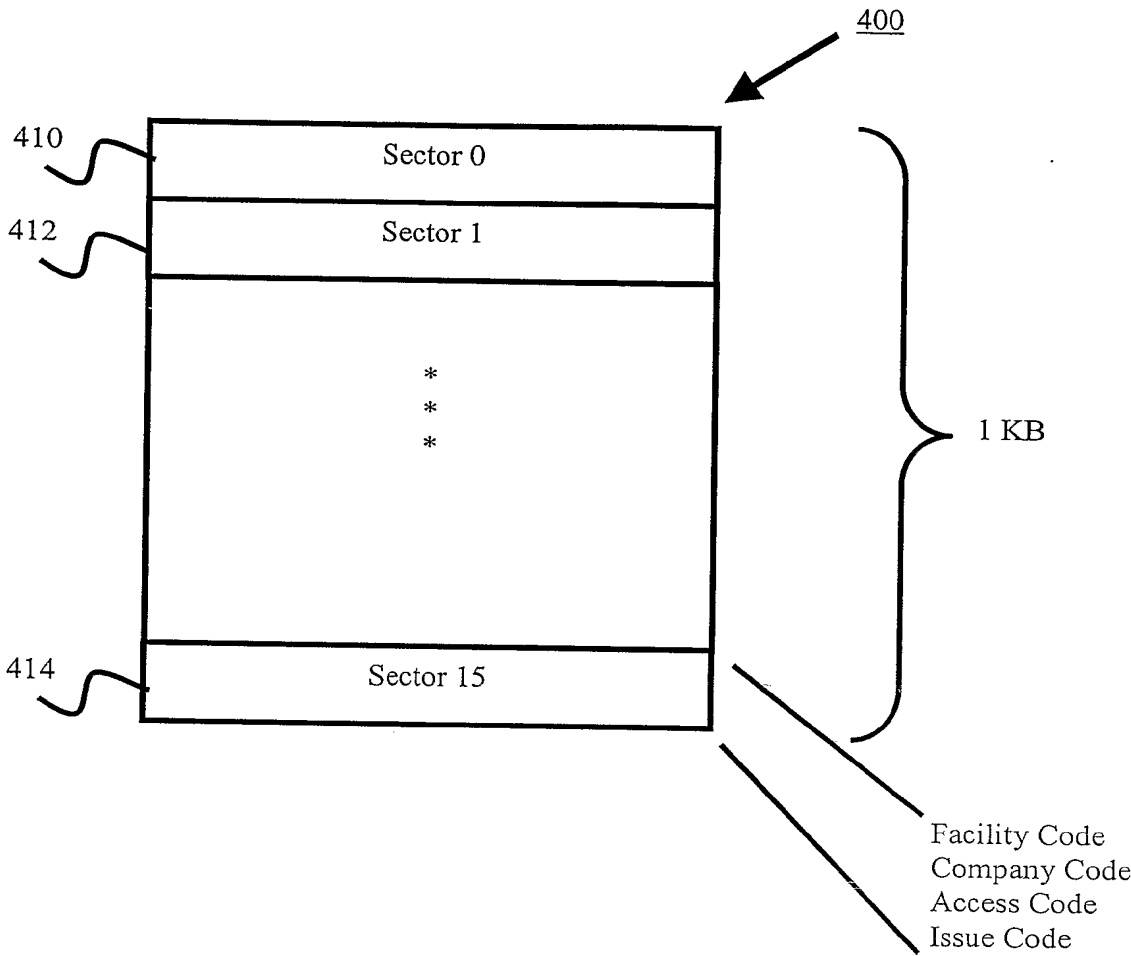


FIG. 4A

<u>Sector</u>	<u>Key A</u>	<u>Key B</u>
0	A0A1A2A3A4 or FFFFFFFFFF	-
*		
*		
*		
15		

450

FIG. 4B

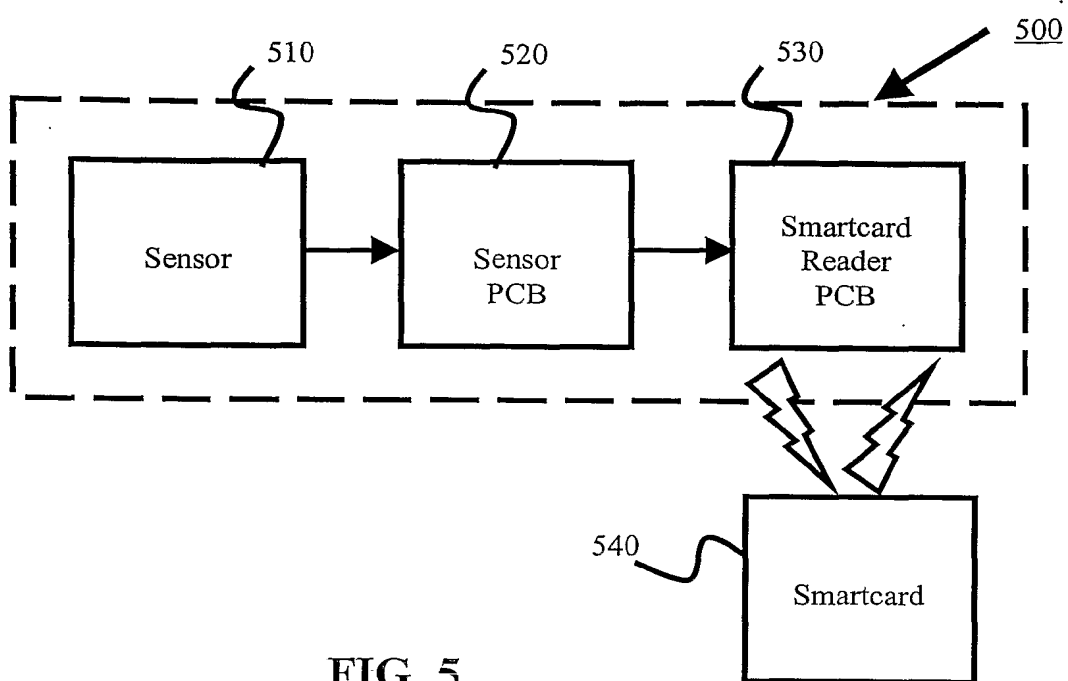


FIG. 5

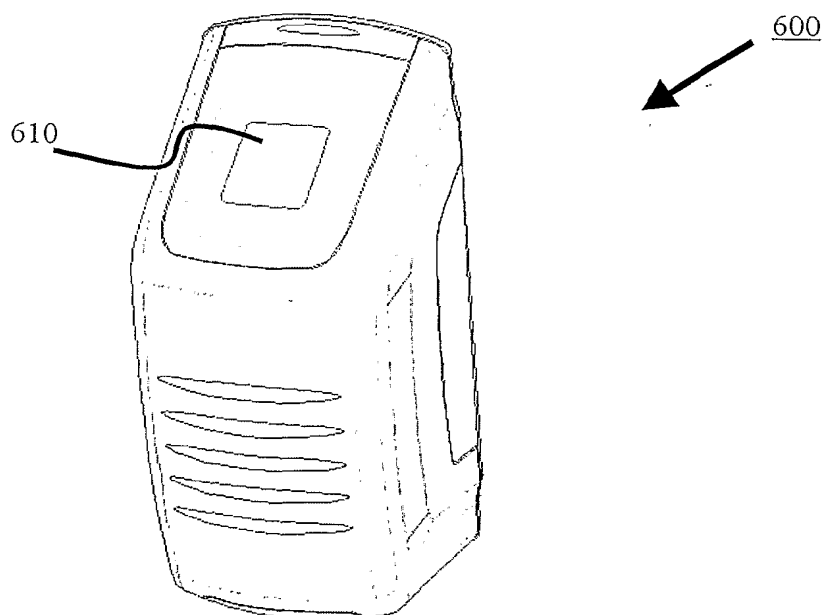


FIG. 6

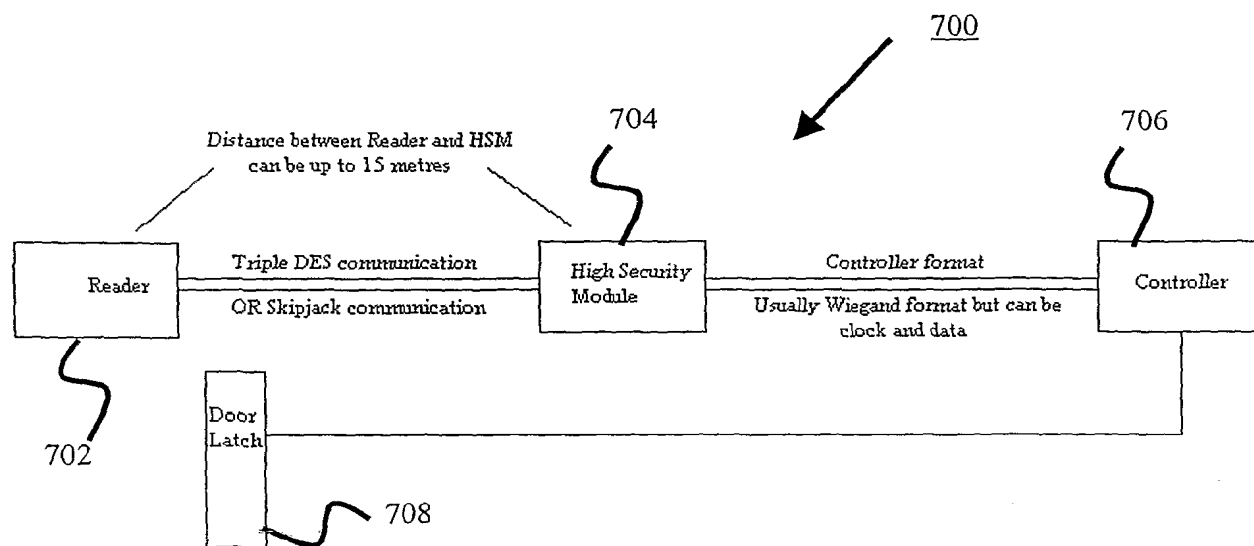


FIG. 7

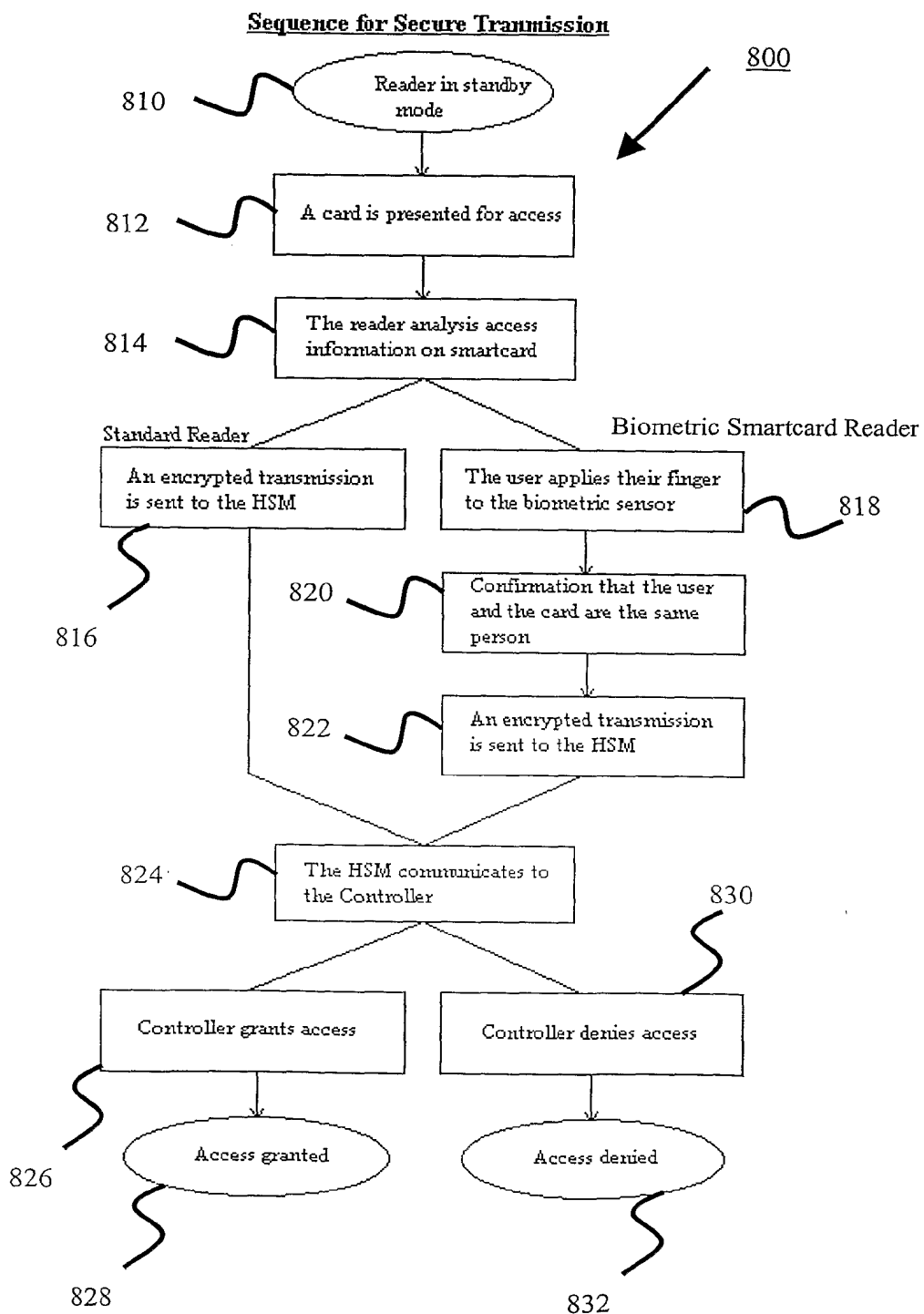


FIG. 8

INTERNATIONAL SEARCH REPORT

International application No.

PCT/AU02/00984

A. CLASSIFICATION OF SUBJECT MATTER												
Int. Cl. ⁷ : G06K 19/07												
According to International Patent Classification (IPC) or to both national classification and IPC												
B. FIELDS SEARCHED												
Minimum documentation searched (classification system followed by classification symbols)												
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched												
Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)												
WPAT: IPC Mark, keywords - smartcard, IC card, chipcard, biometric, fingerprint, secure, verif+, authent+												
C. DOCUMENTS CONSIDERED TO BE RELEVANT												
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.										
X	WO 98/50875A(GTE GOVERNMENT SYSTEMS CORPORATION) 12 November 1998 Entire document	1-14, 16, 17, 19, 20										
X	GB 2 331 825A (NEC CORPORATION) 2 June 1999 Entire document	1-14, 16, 17, 19, 20										
X	EP 0 956 818A (CITICORP DEVELOPMENT CENTER) 17 November 1999 Entire document	1-14, 16, 17, 19, 20										
<input checked="" type="checkbox"/> Further documents are listed in the continuation of Box C <input checked="" type="checkbox"/> See patent family annex												
<p>* Special categories of cited documents:</p> <table border="0"> <tr> <td>"A" document defining the general state of the art which is not considered to be of particular relevance</td> <td>"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention</td> </tr> <tr> <td>"E" earlier application or patent but published on or after the international filing date</td> <td>"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone</td> </tr> <tr> <td>"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)</td> <td>"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art</td> </tr> <tr> <td>"O" document referring to an oral disclosure, use, exhibition or other means</td> <td>"&" document member of the same patent family</td> </tr> <tr> <td>"P" document published prior to the international filing date but later than the priority date claimed</td> <td></td> </tr> </table>			"A" document defining the general state of the art which is not considered to be of particular relevance	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention	"E" earlier application or patent but published on or after the international filing date	"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone	"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art	"O" document referring to an oral disclosure, use, exhibition or other means	"&" document member of the same patent family	"P" document published prior to the international filing date but later than the priority date claimed	
"A" document defining the general state of the art which is not considered to be of particular relevance	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention											
"E" earlier application or patent but published on or after the international filing date	"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone											
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art											
"O" document referring to an oral disclosure, use, exhibition or other means	"&" document member of the same patent family											
"P" document published prior to the international filing date but later than the priority date claimed												
Date of the actual completion of the international search 29 August 2002		Date of mailing of the international search report 02 NOV 2002										
Name and mailing address of the ISA/AU AUSTRALIAN PATENT OFFICE PO BOX 200, WODEN ACT 2606, AUSTRALIA E-mail address: pct@ipaaustralia.gov.au Facsimile No. (02) 6285 3929		Authorized officer JYOTI SHAMDASANI Telephone No : (02) 6283										

INTERNATIONAL SEARCH REPORT

International application No.

PCT/AU02/00984

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 987 155A (DUNN et al.) 16 November 1999 Entire document	1-14, 16, 17, 19, 20
X	GB 2 256 170A (BRANDES) 2 December 1992 Entire document	1-14, 16, 17, 19, 20
X	US 6 219 439B (BURGER) 17 April 2001 Entire document	1-14, 16, 17, 19, 20
X	Derwent Abstract Accession no 2002-007830/01, Class T01, JP 2001 291103A (OKUNO M) 19 October 2001 Abstract	1-14, 16, 17, 19, 20
X	Derwent Abstract Accession No 2001-400687/43, Class T01, JP 2000 311234A (TOKIN CORP) 7 November 2000 Abstract	1-14, 16, 17, 19, 20
X	DE 19924628A (GIESECKE & DEVRIENT GMBH) 30 November 2000 Abstract	1-14, 16, 17, 19, 20
X	WO 02/23796A (SENTRYCOM LTD.) 21 March 2002 Entire document	1-20
X	WO 01/82167A (PHILIPSON, LARS) 1 November 2001 Entire document	1-20
X Y	WO 01/91057A (HARADA et al.) 29 November 2001 Entire document	1-14,16,17,19,20 15 and 18
X Y	GB 2345232A (NDS LTD.) 28 June 2000 Entire document	1-14,16,17,19,20 15 and 18
X	WO 01/08110A (CUBIC CORPORATION) 1 February 2001 Entire document	15 and 18
A	Derwent Abstract Accession No 2000-651521/63, Classes P85;T01, JP2000268145A (MATSUSHITA DENKI SANGYO KK) 29 September 2000 Abstract	15 and 18

INTERNATIONAL SEARCH REPORT

International application No.
PCT/AU02/00984

Box I Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos :
because they relate to subject matter not required to be searched by this Authority, namely:
2. ☐ Claims Nos :
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:
3. ☐ Claims Nos :
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a)

Box II Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

Claims 1-14, 16-17 and 19-20 are directed to a method and apparatus to read a smartcard encoded with biometric data. It is considered that "smart card encoded with biometric data" comprises a first "special technical feature".

Claims 15 and 18 are directed to a method and apparatus to secure transmission from a smartcard reader for encrypting a signal, transmitting said signal to a remote location where transmitted signal is translated to another format and controlling access depending upon the translated signal. It is considered that "the remote controlling of access" comprises a second "special technical feature".

1. ☒ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims
2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.
3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:
4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

- ☐ The additional search fees were accompanied by the applicant's protest.
☐ No protest accompanied the payment of additional search fees.

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/AU02/00984

This Annex lists the known "A" publication level patent family members relating to the patent documents cited in the above-mentioned international search report. The Australian Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

Patent Document Cited in Search Report		Patent Family Member					
WO	9850875	AU	74848/98	BR	9808737	EP	980559
		US	6105010	US	6202151	US	6208746
		US	6310966				
GB	2331825	AU	94222/98	CN	1221160	JP	11161793
EP	956818	US	2001048025				
US	5987155	NONE					
GB	2256170	NONE					
US	6219439	NONE					
JP	2001291103	NONE					
JP	2000311234	NONE					
DE	19924628	AU	200050718	EP	1188151	WO	200074001
WO	200223796	AU	200188679				
WO	200182167	AU	200142946	SE	200001467		
WO	200191057	AU	200124245				
GB	2345232	GB	9909359	IL	126552		
WO	200108110	AU	200040169	EP	1208542		
JP	2000268145	JP	2002073326				
END OF ANNEX							